Network and Information Security Management Discussion Forum

*1 - **Learning Outcomes***

- *Gather and synthesise information from multiple sources (including Internet security alerts and warning sites) to aid in the systematic analysis of security breaches and issues.*

Discussion topic

This discussion is based on the research by Glisson et al's Compromsing a Medical mannequin. We discussed the following questions:

- What are the major threats and vulnerabilities discussed in the paper?
- How would you mitigate against these?

My Initial post

Glisson at al's (2015) research paper Compromising a Medical Mannequin delves into breaching a medical device specifically a production-deployed medial training mannequin. They mention previous governmental and cyber security reports of the health care industry not being prepared for basic cyber intrusion attacks which can have severe impact on patient and medical care.

For their research, they used a virtual environment and a live cd of BackTrack (Reaver), iStan medical mannequin, two laptops, wireless access point, Muse software and a monitor. They found, in a controlled environment, that there were two types of vulnerabilities: the TCP protocol was susceptible to Denial of Service attacks, and the wireless access point was susceptible to brute force attacks.

The vulnerability using BackTrack found was the 802.11 wireless access point WPS (WIFI Protected Setup) PIN which was cracked on both occasions in two hours thirty-eight minutes and seven hours. Gross (2022) highlights several features to mitigate against brute force attacks:

- Locking account after a fixed number of attempts
- Having a delayed response time
- IP address-restricted lock-out
- Use detection tools such as OSSEC
- Brute force scanning.

However, when it comes to WPS brute force attacks specific defences can be implemented. Cisa.gov (2013) advises users to update access point to latest firmware and disable WPS. Further actions to be taken are to use WPA2 encryption with a long alpha-numeric combination, disable uPnP, enable MAC address filtering, restrict unknown computers from the network (www.zyxel.com, 2022).

When it comes to Denial of Service attacks, it seems the best defence is to implement a firewall. In a SYN flood attack, the firewall can impose a limit on SYN requests per second and reroute the extra SYN segments to a queue (www.juniper.net, 2021). Cisa.gov (2019) advises users to enrol in DoS and antivirus software, create a disaster recovery plan, install and configure firewall, and update security practices.

Response from Beran:

Hi Jonathan,

I enjoyed reading your initial post. I think you have concisely considered the main vulnerabilities the article mentioned, of both DOS and brute force attacks, and I enjoyed your explanation of them.

These attacks were implemented using common tools, such as HPING3 for the DOS attack and Reaver for the Brute force attack. Reaver, and other tools such as WPSCrack, can be part of a standardised approach for vulnerability testing.

Although these tools are extremely useful for testing the vulnerability of a system, what are your thoughts regarding their ease of access? Do you believe that it is of great concern that such easily accessible tools can be applied to exploit vulnerabilities as mentioned in the "Compromising a medical mannequin" (Glisson et al., 2015) case study?

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth).

Response From Agne:

Hi Jonathan,

thank you for sharing your thoughts on the paper with us.

In your overview on mitigation against brute force attacks on the WPS vulnerability discussed in the paper on Medical mannequin (Andel et al, 2015), you mentioned disabling the Universal Plug and Play (UPnP) protocol within the router. The UPnP is often used for heavy port forwarding environments due to its useful feature of auto port forwarding, so it's quite useful when you have many computers on IoT trying to access private local-area network (Wherry, 2022), for example, education environments where off campus/facility students require access to their campus/network.

So, depending on what other devices use the same router to which the iStan mannequin is connected and whether remote access to it is required, it may be more beneficial having the UPnP turned on. Do you think the benefits of auto port forwarding provided by the UPnP outweigh the security risks associated to it or would you rather disable the UPnP and configure the port forwarding rules manually?

References

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth).

Wherry, J. (2022) What is port forwarding and how safe is it? Available from: https://cybernews.com/what-is-vpn/port-forwarding/ [Accessed 15 March 2022].

My response to Agne:

Hi Agne,

Thank you for your reply.

I totally agree with you regarding the benefits of UPnP for heavy port forwarding especially in the example of off campus/facility students needing access to their campus network. Over the last ten years most of the vulnerabilities of UPnP have been patched. For example, gamers using Xbox and PlayStation consoles may find it beneficial to enable UPnP for ease of use. One advantage to this is the console is 'locked down'; only games and related stuff can be downloaded from the official vendor store. Therefore, there is very low probability of getting malicious software that can spread throughout the network (Oliver, 2022).

Nevertheless, there are still some issues with using UPnP. Carnegie Mellon University (CMU) and the National Institute of Standards and Technology (NIST) lists Common Vulnerability Exposures (CVEs) regarding UPnP. Two vulnerabilities highlighted by CMU are VU#339275, 357851. VU#339275 can abuse the UPnP Subscribe function to send large amounts of data to trusted devices on the network causing a DDoS attack (Sarvepalli, 2020). VU#357851 can allow UPnP requests over the WAN interface connecting to internal hosts behind the firewall such as UPnP mapping attacks (Allar, 2012).

It seems the UPnP protocol is relatively safe if secured, and safe devices are on the network. I believe it is better to disable certain features and protocols if not being used and if security can be improved though manual configuration; however, misconfiguration is always an issue.

Do you have a personal or professional preference?

References

Allar, J. (2012) CERT/CC Vulnerability Note VU#357851. www.kb.cert.org. Available from: https://www.kb.cert.org/vuls/id/357851/ [Accessed 17 Mar. 2022].

Oliver (2022) Port Forwarding vs DMZ vs UPnP For Gaming (Complete Guide). Weak Wi-Fi Solutions. Available from: https://weakwifisolutions.com/port-forwarding-vs-dmz-vs-upnp-for-gaming/ [Accessed 17 Mar. 2022].

Second response from Agne:

Hi Jonny,

I agree with you; provided an up to date UPnP protocol is implemented, the devices on the network don't contain additional vulnerabilities, the data shared on the network is not secret or confidential, the implementation of UPnP can provide many benefits.

However, a risk analysis on whether an already implemented UPnP protocol should be kept or one should be implemented should certainly be conducted, since the users are not only exposed to the DOS or mapping attacks, but also to information leakage (MAC address, serial number, device model) and command execution on devices (Garcia, 2019).

I think it is important to not blindly implement new policies or vulnerability mitigation techniques based on reported vulnerabilities. Disabling the UPnP could be detrimental to one business, or it could be the most sensible thing to do for another. However, security specialists won't know that until they understand the network they are working with, the devices on the network and their associated vulnerabilities, the business case for UPnP, etc.

References:

Garcia, D. (2019) DefCon: UPnP Mapping. Available from: https://toor.do/DEFCON-19-Garcia-UPnP-Mapping-WP.pdf [Accessed 21 March 2022].

Response from Andrijana:

Hi Jonathan,

Thank you for your contribution to the discussion, I enjoyed reading your post!

Brute force and DoS attacks discussed in the paper can indeed be damaging to the medical field. I agree with your mitigation suggestions and would like to add that choosing a secure password could also help reduce the risk of brute force attacks. For example, to create an account nowadays it is most likely to stumble upon password requirements, such as minimum length, must include at least one number, one symbol and/or one capitalised letter. Brecht (2021) suggests that establishing a secure password, the password itself must be lengthy and complex, as the combination of the two will make it less likely to break. The complexity of the password could be the addition of capitalised letters, punctuation or misspellings (Brecht, 2021).

Another suggestion to mitigate a brute-force attack could be the implementation of a two-factor authentication (2FA). 2FA offers an additional layer of security to the account and therefore even if the password is retrieved by the attacker, the attacker would still need the second source of verification (WP SitePlan, 2022).

References:

Brecht, D. (2021) Password security: Complexity vs. length. Available from: https://resources.infosecinstitute.com/topic/password-security-complexity-vs-length/ [Accessed 16 March 2022].

WP SitePlan (2022) What are Brute Force Attacks - And How Can You Prevent Them? Available from: https://wpsiteplan.com/blog/what-are-brute-force-attacks/ [Accessed 16 March 2022].

Response from Ali:

Hi Jonathan,

I enjoyed reading your post.

The article Compromising a Medical Mannequin by Glisson et al. (2015) focuses on breaking production-deployed medial teaching mannequin. I agree with the research findings that the health care industry is unprepared for simple cyber intrusion attempts, which can have severe consequences for patients and medical services. With the industry's growing dependence on information technology (IT), cyber-criminals are increasingly targeting and profiting on hospital vulnerabilities (Muthuppalaniappan and Stevenson 2021, p.4). Consequently, healthcare professionals and organizations must demonstrate an awareness of cybersecurity and ensure they are protected and prepared to respond in case of any form of cyber-attack. Unfortunately, healthcare companies frequently lack the resources to defend themselves against cyber-attacks and can be severely impacted by the cost and long-term consequences of security breaches (Muthuppalaniappan and Stevenson 2021, p.5). In addition, several Internet of Things (IoT) equipment is susceptible to cyber-attacks mainly because healthcare gadgets are either inadequately protected against potential threats or not safeguarded (Yaacoub et al 2020, p. 581). Any cyber-attack might have disastrous implications thus endangering patients' lives and impeding the widespread use of these tools. In addition, cyber attacks may have consequences thus putting patients' lives at risk and limiting the use of these instruments.

Furthermore, the research highlights two principal vulnerabilities in a controlled environment, including Denial-of-Service attacks and brute force assaults. As such, organizations in the health care sector can employ threat intelligence technologies and artificial intelligence algorithms to mitigate these risks and boost security (Ranganayaki et al 2020, p.94). Additionally, Moudoud, Khoukhi, and Cherkaoui (2020, p.198) propose a cybersecurity system based on a Markov stochastic process used to watch each network device's behavior and employs a range-based behavior filtering strategy. Hospitals can employ this system to secure themselves against these attacks. Furthermore, hospitals can be secured against brute force attacks by establishing virtual patching applications to identify malicious traffic before it reaches the susceptible device. In addition, organizations can mitigate these risks by deactivating Internet control message protocol requests on edge nodes. The edge nodes might be set to block any IP address within the healthcare domain (Bradley, El-Tawab and Heydari 2018, p.150).

References

Bradley, C., El-Tawab, S. and Heydari, M.H., 2018, April. Security analysis of an IoT system used for indoor localization in healthcare facilities. In *2018 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 147-152). IEEE.

Moudoud, H., Khoukhi, L. and Cherkaoui, S., 2020. Prediction and detection of fdia and ddos attacks in 5g enabled iot. *IEEE Network*, *35*(2), pp.194-201.

Muthuppalaniappan, M. and Stevenson, K., 2021. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), p.mzaa117.

Ranganayaki, R.S., Sreeja, B., Gandhari, S., Ranganath, P.T. and Kumar, S., 2021, December. Cyber Security in Smart Hospitals: A Investigational Case Study. In *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)* (pp. 92-98). IEEE.

Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R. and Chehab, A., 2020. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Generation Computer Systems*, *105*, pp.581-606.

Beran's post

Hi Everyone,

Firstly, thanks very much to all of you for such a productive and active discussion forum - obviously the points raised in the paper struck many chords with you all. I look forward to read your summary posts as you add them this week.

From the point of view of the computer systems used for monitoring and configuration - I think there is very little for me to add. Many people made some excellent points about how to lock down the network and the use of AV, firewall, and IDS/IPS systems - all of which I think that medical services should take on board.

However, it is in the domain of embedded devices - the so-called Internet of Things (IoT) that the need for innovation and new solutions lies. The recent pandemic has demonstrated that the increasing number of electronic devices used for monitoring, managing, and ameliorating medical conditions absolutely need to be low maintenance, reliable and as immune to attack as possible. Unfortunately, all such devices will need interventions from time to time - whether it is basic monitoring, resynchronising clocks, or carrying out software patching or updates, all such devices need a means of remote access. Performing surgery to access these devices is too expensive, time-consuming and in many cases introduces unneeded risks to the patient. However, as the many posts here attest, wireless communication is also fraught with risks and dangers.

As cybersecurity specialists of the (near) future, we should regard this as one of the challenges of our field - cybersecurity is a big challenge in the IoT domain and we should be looking at new and innovative methods of securing these most vulnerable of devices.

For example - can we use blockchain programming techniques to make the communication links more secure? Many IoT devices use mesh networking because they have low power, limited range radios on-board. Is there any way of utilising mesh networking techniques to also secure the network? Several people made some very good recommendations around locking down MAC addresses but should we still be looking at that level? Can IPv6, SDN, and VNFs be explored as alternative ways of addressing and securing such devices?

We will touch on a few of these topics later in the module, and I encourage those of you with an interest in the more technical areas of networking and cybersecurity to start thinking about investigating some of these topics as the subject of your master's project.

Regards, Beran.

My response to Beran:

Hi Beran,

It was interesting to read your example on blockchain programming techniques and IoT.

Similar to blockchain technology, Internet of Things has also proliferated to such an extent that around 50-Billion devices will be owned this decade. However, their popularity has come at a cost. Vulnerabilities are common has manufactures seek to make inexpensive and easy to use devices such as a locked default username and password (Fakhri and Mutijarsa, 2018).

Since Satoshi Nakamoto started to use blockchain technology for Bitcoin, it has spread into other fields such as cryptocurrency, healthcare, and logistics. Other types include Ethereum blockchain and smart contracts. (Fakhri and Mutijarsa, 2018).

There are four main features of blockchain technology:

1. It is decentralised. Third parties do not need to very transactions.
2. It is persistent. Transactions can be validated and cannot be deleted once transacted.
3. It is anonymous. Users are hidden behind a generated address.
4. It is auditable. Transactions can be easily tracked and verified.

According to Fakhri and Mutijarsa's research (2018), they used to two systems: with blockchain and without blockchain. One system used standard Message Queueing Telemetry Transport (MQTT) broker protocol running TCP/IP, and the data encrypted and hashed using AES and SHA-256. The second system used an Ethereum blockchain, ECDSA encryption AND Keecak-256 Hash.

From their findings and attack simulations, they concluded that IoT using blockchain technology was more secure as its data integrity was guaranteed.

References

Fakhri, D. and Mutijarsa, K. (2018) Secure IoT Communication using Blockchain Technology. *2018 International Symposium on Electronics and Smart Devices (ISESD)*.

My summary

50 billion IoT devices are expect to operational by 2024 ranging from simple home security devices to complex medical training iStan mannequins. Yet, these devices are poorly configured and lacking even basic authorisation protocols such as changing the username and password (Fakhri, D. and Mutijarsa, K.,2018).

Glisson et al's research paper (2015) highlighted the ease attackers can use basic penetration tools such as BackTrack (Reaver) to scan for vulnerabilities and exploit the iStan medical devices; the TCP protocol was susceptible to Denial-of-service attacks and the WPS PIN was cracked.

Certain mitigation strategies can be used to secure the network and medical devices including disabling UPnP and WPS, implementing VLANS, using passive and active scanning tools. Angelides (2022) mentioned conducting a risk analysis on the UPnP protocol to further understand the organisation's need for it , and Klacar (2022) suggested using a complex twelve-digit password to enforce against brute force attacks.

However, there is another modern tool that can greatly improve IoT security as suggested by Necat (2022): blockchain technology. There are four main tenets of blockchain technology:

1. It is decentralised. Third parties do not need to verify transactions.
2. It is persistent. Transactions can be validated and cannot be deleted once transacted.
3. It is anonymous. Users are hidden behind a generated address.
4. It is auditable. Transactions can be easily tracked and verified.

Research by Fakhri and Mutijarsa (2018) highlighted IoT devices using blockchain technologies were vastly more secure than traditional standard Message Queueing Telemetry Transport (MQTT) broker protocol running TCP/IP.

It seems that IoT devices are an integral apart of modern life either professionally or personally; however, manufactures are producing many unsecured and vulnerable devices which can be exploited by even novice attackers. Conducting a Risk, DREAD, and STRIDE analyses can help to better implement relevant mitigation strategies; conversely, this is may not be a viable approach for the average consumer.

References

Angelides, A. (2022) Peer response. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=299733 [Accessed 27th March 2022]

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth).

Fakhri, D. and Mutijarsa, K. (2018) Secure IoT Communication using Blockchain Technology. *2018 International Symposium on Electronics and Smart Devices (ISESD)*.

Klacar, A. (2022) Peer response. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=299733 [Accessed 27th March 2022]

Necat, B., (2022) *Summary Post* Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=301666 [Accessed 27th March 2022]